

JWT

JSON Web Token

Qu'est-ce qu'un token ?

- **Facteur d'authentification de possession** (on **possède** un token mais on ne le connaît pas par cœur...)
- Généralement associé à un ensemble de permissions dont dispose un utilisateur (de par son rôle ou ses informations)

Pourquoi privilégier le token au mot de passe ?

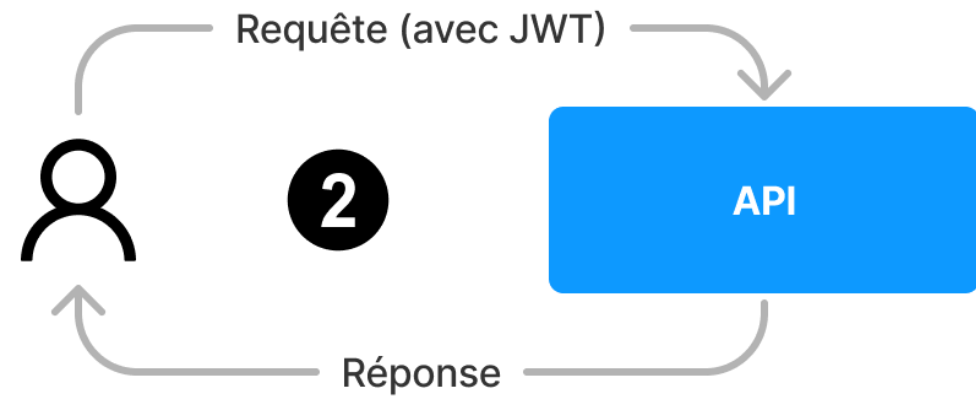
- Créer plusieurs token qui ont des **ensembles** de permissions différents
- Si un token est compromis, seules les permissions associées sont compromises
 - À l'inverse, si un mot de passe utilisateur est compromis, c'est **l'ensemble** des permissions liées à cet utilisateur qui sont compromises

Clé d'API (API key)

- Une clé d'API est un type de token permettant d'accéder à une ressource
- Ce token fait office de **clé** permettant de "déverrouiller" l'accès à une API

JWT (JSON Web Token)

- [RFC 7519: JSON Web Token \(JWT\)](#)
- **Standard** très largement utilisé dans l'authentification sur le Web
- Simple à utiliser



Fonctionnement du JWT

<https://jwt.io/>

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MzQyNTY2Mj0uSf1KxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

Thu Jan 18 2018 02:30:22 GMT+0100 (heure normale d'Europe centrale)

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

Confiance

- Comment **authentifier** un JWT ?
- Grâce à un système **crypto** de **signature** (HMAC)